ESD-TR-77-256

MTR-3440

AUTOMATIC JAMMER LOCATION TECHNIQUES

NOVEMBER 1977

Prepared for

DEPUTY FOR DEVELOPMENT PLANS
ELECTRONIC SYSTEMS DIVISION
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
Hanscom Air Force Base, Bedford, Massachusetts

Project No. 6740
Prepared by
THE MITRE CORPORATION
Bedford, Massachusetts
Contract No. AF19628-77-C-0001

REVIEW AND APPROVAL

This technical report has been reviewed and is approved for publication.

Thomas F. Brownell

THOMAS F. BROWNELL, Major, USAF
Project Engineer

FOR THE COMMANDER

Michael H. Alexander

MICHAEL H. ALEXANDER, Col, USAF
Deputy for Development Plans

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: ESD-TR-77-256	2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER	
4. TITLE (and Subtitle): AUTOMATIC JAMMER LOCATION TECHNIQUES	5. TYPE OF REPORT & PERIOD COVERED
	6. PERFORMING ORG. REPORT NUMBER: MTR-3440
7. AUTHOR(s): R.W. Jacobus, A. Bark	8. CONTRACT OR GRANT NUMBER(s): AF19628-77-C-0001
9. PERFORMING ORGANIZATION NAME AND ADDRESS: The MITRE Corporation, Box 208, Bedford, MA 01730	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: Project No. 6740
11. CONTROLLING OFFICE NAME AND ADDRESS: Deputy for Development Plans, Electronic Systems Division (AFSC), Hanscom Air Force Base, MA 01731	12. REPORT DATE: NOVEMBER 1977
	13. NUMBER OF PAGES: 62
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)	15. SECURITY CLASS. (of this report): UNCLASSIFIED
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

ANTENNAS
DIRECTION FINDING
JAMMER LOCATION
STROBES

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This document surveys passive methods for determining the locations of airborne jammers from ground-based radar surveillance sites, and examines the prospects for supporting fully automatic measurements. The performance of these methods when confronted with noise jammers of various levels of sophistication is discussed. The techniques are compared in terms of effectiveness and complexity to provide a

(over)

20. ABSTRACT (Continued)

guide for the design of ECCM subsystems associated with track-while-scan radar surveillance networks.

ACKNOWLEDGMENTS

This report has been prepared by The MITRE Corporation under Project No. 6740. The contract is sponsored by the Electronic Systems Division, Air Force Systems Command, Hanscom Air Force Base, Massachusetts.

TABLE OF CONTENTS

		Page
LIST OF FIGURES		4
SECTION I	INTRODUCTION	5
SECTION II	BASIC JAMMING THREATS	17
SECTION III	DIRECTION-FINDING AND JAMMER-LOCATION TECHNIQUES	25
SECTION IV	SYSTEMS VERSUS THREATS	50
SECTION V	SUMMARY AND CONCLUSIONS	59

LIST OF FIGURES

Figure Number		Page
1	Location of Jammers by Triangulation	10
2	Several Typical ECCM Displays	14
3	Randomly-Modulated Jamming	22
4	Scan-Synchronized Jamming	22
5	Example of Cooperative Jamming	24
6	Direction-Finding Equipment for System No. 1	27
7	Direction-Finding Equipment for System No. 2	30
8	Direction-Finding Equipment for Systems No. 3 and 4	33
9	Part of Equipment for Direction-Finding System No. 5	39
10	Block Diagram of Bistatic Correlation System No. 6	42
11	Block Diagram for Single-Beam Correlator	43
12	Directional Anti-Correlation Jamming	46
13	"Distributed" Anti-Correlation Jamming	46
14	Rotating Dual-Antenna Assembly for Direction Finding	49
15	Performance of Various Systems vs. Amplitude-Modulated Noise Jammers	51

SECTION I

INTRODUCTION

The problem addressed in this report is that of passively measuring the locations of airborne jammers which are operating against a network of ground-based surveillance radars. This is the converse of the usual problem, in which active radars are attempting to detect targets in spite of enemy jamming.

The location of airborne jammers can be important to tactical and strategic operations. In many cases, attacking enemy aircraft will use jamming as a means of self-defense; by locating the source of jamming, we can guide our intercept aircraft into a position where their own fire-control systems become effective. Similar notions apply to "escort" jammers which fly along with a formation of attacking aircraft. In other cases, powerful long-range jammers might orbit in a "standoff" mode; location of their approximate positions will permit the use of correspondingly long-range weapons (e.g., cruise missiles). The location and tracking of jammers can provide information about the number of aircraft and the intent of an attacking wave. In general, the enemy reveals something about himself whenever he decides to radiate jamming signals, and a jammer-location system is an attempt to exploit that information.

It is a curious fact that the jammer-location problem has not been adequately treated, despite more than 20 years of operational experience with radar surveillance networks in this country. The general approach

has been to rely heavily on manually operated visual displays. The performance of the systems against jammers has been rather poor, and in most cases only the simplest type of jamming has been used in tests. Now, after all these years, the basic problems are still formidable, the tested operational approaches are wholely inadequate against modern sophisticated threats, and the conceptual approaches have not been studied adequately or subjected to any real explorative testing.

This report does not attempt to solve all these problems and or to advance the state of the art. Rather, we wish to survey modern jamming threats and techniques for jammer-location; in some cases we will suggest approaches which, so far as we are aware, have not been studied previously. We will identify areas where more study and field-testing is necessary. One purpose of the report is to "rank" jammer-finding techniques against the sophistication of the jammers, so that a radar system designer can more readily select his approach on the basis of the threat-sophistication he feels is realistic.

Unfortunately, a complete treatment of even this limited area is beyond the scope of the report. We will focus our attention on noise jammers, i.e., jammers whose radiated waveform approximates a sample of band-limited random white noise. This class of jammer is still the most common, even in modern times, because it is the only fundamentally reliable way to jam a radar receiver. Any radar system, regardless of its complexity and sophistication, can be rendered useless by a sufficient quantity of random noise injected into the receiver

(so long as the noise covers the radar's passband). It is only necessary for the enemy to assure himself that the strength of the noise is adequate to the task; he need not be concerned with the details of the radar's design. With this type of jamming, directed against a conventional monostatic radar, most or all of the detection cells of the radar will be filled with jamming noise, along the azimuth of the jammer. The radar will then be unable to detect the jammer--or any other target at that azimuth--on the basis of reflected radar energy; i.e., the radar will be unable to measure the range of any target along the jammer's azimuth. Early radars which used a polar Plan Position Indicator (PPI) display of the receiver's output would show a bright line at the azimuth of the jammer, indicating a general increase in the noise level at that point. This bright line was called a "strobe", and we will occasionally use the term later. However, modern radars almost always utilize Constant False Alarm Rate (CFAR) circuits to maintain a constant noise level at the receiver's output, and strobes are no longer normally seen on the radar displays.

There are many types of jamming other than simple noise-modulation. They include sweep jamming, pulse jamming, and "spoofing" or decoy jamming. When the jammer design is optimally matched to the specific radar against which it is intended to operate, these other types of jamming can be far more efficient than noise. Generally they produce false targets in the radar's output, and either exceed the ability of the radar post-processor to filter out the real detections from the

false ones, or emulate real targets with sufficient accuracy that the radar operators are deceived into treating false targets as real ones (e.g., by sending out interceptors in the wrong directions). However, the ability of the non-noise jammer to disable a given radar is a sensitive function of the radar's design and the precise form of the jammer's waveform.

For our purposes here, jammers other than the noise type are too complicated for consideration in an initial survey. Jammer location is difficult at best, and it is especially troublesome if there are no constraints at all on the jammer's waveform or duty cycle. This suggests that a jammer would be at an advantage if he uses decoy or spoofing techniques; while there is no question that these non-noise techniques are optimal if they are successful, they also pose a severe danger to the jammer if his transmissions are not a sufficiently credible simulation of the radar's signals. In other words, noise jamming is not always efficient, but is almost completely predictable in its effects, while decoy jamming may be efficient but unpredictable. Hence noise jamming is still a popular approach, and deserves the special attention it receives in this report.

General Basis for Jammer Location

When an enemy jams a radar using noise, the radar can sense an increase in received power at an azimuth corresponding to the location of the jammer. Thus a single radar can sense the azimuthal direction of the jammer, but cannot in general determine the jammer's range.

It should be noted that airborne surveillance systems can sometimes employ multipath reflections from ground terrain to get a rough estimate of a jammer's range; the technique involves measurement of the delay between two versions of the received jamming signal.

Two or more receiving sites with overlapping coverage may be used to triangulate on a jammer. When the geometrical relationships are favorable, a jammer may be located with considerable precision, and his motion may be tracked passively in the same manner as is done with conventional skin-painted targets.

If two or more jammers are successful in jamming all of the surveillance radars in their coverage region, then the process of triangulation can still be employed, but ambiguous or false strobe-intersections are introduced because the receiving sites cannot uniquely associate each jammer with its corresponding strobe. For example, with two jammers and two receiving sites, two additional "ghost" jammers are indicated by triangulation, as shown in Figure 1. In general, N jammers will produce $N^2 - N$ ghosts when viewed from two receiving sites.

Ghost-jammers can be distinguished from actual jammers by a variety of methods, none of which is entirely satisfactory. First, all strobe intersections can be tracked by a computer, and the tracks can be examined for "authentic" aircraft behavior; e.g., in some cases a false track can be detected because it appears to be moving too fast, or accelerating too rapidly, for a real enemy airplane. The apparent motion of the intersections can, of course, be used to decide the priorities of aggressive

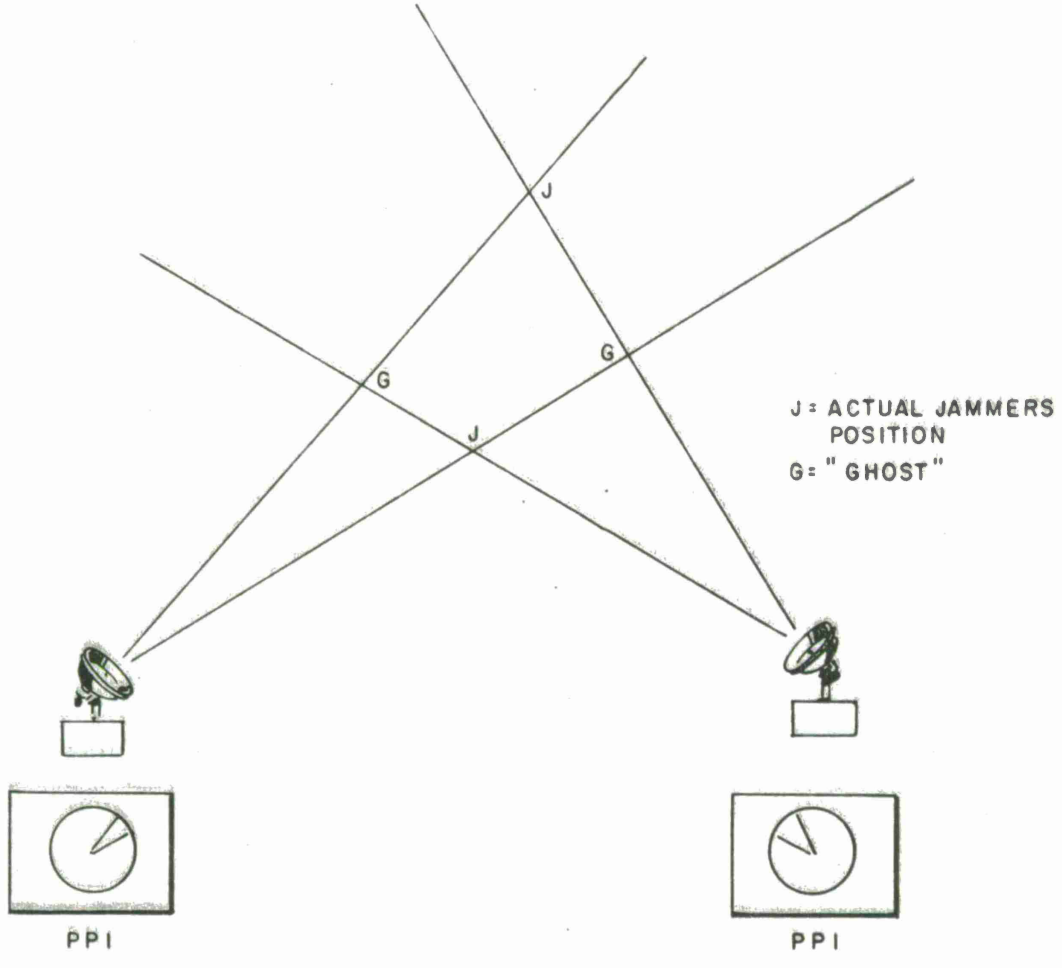


Figure 1. LOCATION OF JAMMERS BY TRIANGULATION

actions--intersections which appear to be moving away from the receiving sites might be regarded as less threatening. A second method is to consider the time-order in which jammers appear at the receiving sites, either because formerly silent jammers turn on, or because they approach over the local horizon of the sites. If several jammers appear one at a time, it is often possible to sort out the true strobe-intersections from the false. A third technique for removing or reducing ghosts is to equip each receiving site with processors that can search for unique "tags" in the jammer signals. For example, the spectrum of one jammer may be slightly different in width or uniformity from a neighboring jammer's; if these clues or tags can be detected reliably at all of the sites, then the extra information can be very helpful in sorting out the false intersections.

All of the methods mentioned above utilize azimuth measurements (perhaps supplemented by other data) to locate the positions of jammers. Consequently, in this report we shall emphasize the problem of making accurate unambiguous azimuth measurements from a single site, and we shall assume that the azimuth data are combined in some fashion to yield jammer location.

Theoretically there are several ways to combine the RF, IF, or video signals collected at two or more sites to locate jammers in both azimuth and range. One such method[1] is to coherently interconnect three receiving sites so that the curvature in the jammer's RF wavefront can be estimated (thereby yielding an approximation to range). In practice,

[1] R.W. Jacobus, "The Interferometer," Technical Report No. 232, Lincoln Laboratory, 22 September 1960.

only one multistatic technique has thus far shown any real promise: cross-correlation of jamming signals received at two sites. This will be the only system in our subsequent discussions which can measure the locations of jammers in two dimensions.

Automation

The location of jammers has traditionally been performed with a mixture of manual and computer-sided operations. For example, in the SAGE system (circa 1960) an operator in an individual radar site manually designated* azimuthal regions where he believed jammers were to be found (i.e., he made coarse decisions, for the purpose of removing ambiguities); the local site computer measured the azimuths of the jammers by "beam-splitting" in the azimuth domain; the azimuthal data were sent from each radar site to the control site; the computer at the central site displayed the intersecting jamming-strobes on a common coordinate system; finally, an operator designated any of the intersections for subsequent tracking by the computer. The local site operators were essential to the process because, without their manual intervention, either most of the jammers would go undetected or an intolerable number of false azimuth-reports would be generated.

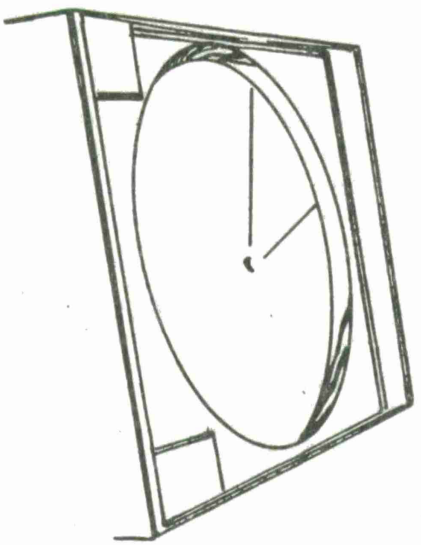
Completely automatic operation, especially at the local sites, is strongly desired in the design of a modern radar system. The primary

*For this purpose a special polar display of power-versus-azimuth was used, in an ECCM processor called a Threshold Control Unit[1].

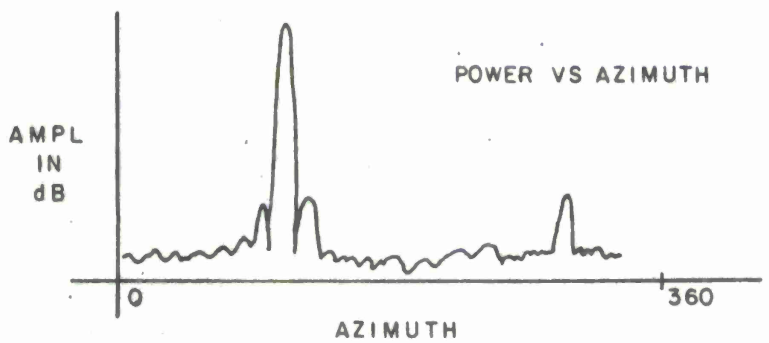
motive is the potential for reducing operating and maintainence costs by eliminating as many humans as possible from a given site, or by avoiding the need for highly trained operators. A secondary attraction is the possibility for improved performance; in principle, a machine can respond faster and more accurately to the rapidly-changing ECM environment which may be encountered in modern war.

The conventional display equipment at a site allows the operator to see a plot of average received power versus azimuth (sometimes presented in polar form). Point targets detected by the radar have low power compared with receiver noise averaged over an azimuthal resolution call, but noise introduced by jammers is prominent, as shown in Figure 2. Each individual jammer causes a reproduction of the receiver's antenna pattern to be plotted on such a display. If the jammers are well separated in azimuth and are of roughly equal strength, then an operator will have no difficulty in distinguishing and counting the jammers, and in estimating their azimuths. When the jammers are close together in azimuth and/or have widely disparate signal power, some of the small jammers will be lost in the sidelobes of the larger ones, the sidelobes of some large jammers might be mistaken for small jammers, and the peak-power regions might not always correspond to the true locations of the jammers.

When a human operator is confronted with this problem, he can often perform surprisingly well in spite of the confusions inherent in the display. He uses talents which are natural and instinctive to



PPI
LIMITED DYNAMIC RANGE



POWER VS AZIMUTH
(POLAR DISPLAY)

Figure 2. SEVERAL TYPICAL ECCM DISPLAYS

a human, but which are likely to be rather difficult to emulate in a machine. First, he tries to make optimum use of the time-ordered sequence in which the jamming signals appear at the local site. In the usual type of operational jamming exercises, the radar might be attacked by many different jammers, but they seldom all turn on at once (alternatively, they might not all come over the site's local radio horizon at the same time). Second, he trains himself to look for familiar patterns; he learns to recognize the shape of the receiving antenna's pattern, and can visualize and sort out superpositions of several identical patterns which are shifted in azimuth and altered in size. Third, he uses common sense in his attempts to pick out tactically reasonable groupings of jammers.

A machine can be designed to estimate the peak of a function--i.e., to beam-split--better than a human operator, and the procedures for doing this are well established. The other talents attributed to humans in the discussion above can also be implemented in a machine, but the algorithms are not available (except for simple situations), and a good deal of development and experimentation will be required before a machine can surpass a human operator in this arena.

The attributes of pattern recognition and common sense are essential ingredients to a system which must extract the desired data from a presentation of power versus azimuth. As will be described later, there are several potential approaches to jammer location which are not limited to power measurements alone; they utilize both amplitude and phase measure-

ments, or the equivalent information inherent in the correlation of IF waveforms. These approaches do not, in general, yield the ambiguous results of the power-only methods, and presumably would not require sophisticated software to make them suitable for wholly automatic operation.

Summary

The remainder of this document will deal with the limited case of noise jammers operating against a single ground-based surveillance radar, which is assumed to be part of a network of overlapping sensors. For most of the jammer-location techniques under consideration, the goal is the accurate unambiguous measurement of jammer azimuth from the receiving site; one of the techniques (involving bistatic measurements) is capable of locating jammers in both range and azimuth. As noted above, the measurement of jammer azimuth is only one portion of the total task, but we will not discuss further the remaining operations of deghosting the complex set of intersecting strobes, and finding unique "tags" or signatures which will help the deghosting process.

Section II will discuss the basic noise-jamming threats and the way in which they interact with conventional radars. Section III will survey the techniques which can be used to measure the azimuth of jammers from a single receiving site, or the azimuth and range from a bistatic receiving configuration. Section IV will present a matrix of measuring techniques versus jamming threats, and will discuss the ramifications of each combination.

SECTION II

BASIC JAMMING THREATS

When a single noise jammer confronts a conventional mechanically scanned radar, a variety of effects may be produced, but in general the radar receiver will observe a maximum in the received noise power at the azimuthal direction of the jammer. If the jamming signal is very weak, the radar may still be capable of detecting radar pulses reflected from the jammer, and thus may determine both range and azimuth of the enemy.

The pattern of power versus azimuth observed by the radar is a direct measure of the effective one-way pattern of the radar's receiving antenna. If the sidelobes of the radar antenna are extremely small compared to the main lobe, then a typical jammer will interfere with the radar only in the immediate angular vicinity of the jammer's true azimuth. If, on the other hand, the radar's antenna sidelobes are not very small and/or the jammer is exceptionally powerful, then the jammer can inject appreciable power into the radar receiver at all azimuths--even through the "far" sidelobes and backlobes of the antenna. In the latter situation, we must be concerned with the entire 360° antenna pattern, and not simply that portion of it near the main lobe.

Our primary interest in this report is with ground-based surveillance systems. The proximity of the sensor antennas to ground terrain introduces two factors which tend to complicate the jammer-location problem. Although it is now within the state-of-the-art to fabricate

antennas having exceedingly low average sidelobes, the effective patterns of these antennas when installed at a typical ground site are often much degraded by the presence of indirect reflections from neighboring hills, vegetation, water towers, power transmission lines, and buildings. Consequently, the effective sidelobes of a ground-based system are seldom much lower than 25 dB below the peak gain of the antenna, and it is relatively easy for an airborne jammer to inject noise into the radar from all azimuths. The second factor, which makes the pattern-recognition approach rather difficult, is the change in the effective antenna pattern as the antenna aperture is scanned; i.e., the influence of local terrain on the pattern is a function of the direction in which the antenna is pointing. Thus techniques which attempt to store a carefully measured replica of the antenna pattern can sometimes fail because the actual real-world pattern does not remain constant.

Now let us consider the straightforward case of multiple noise-jammers, each transmitting at an arbitrary but constant power. The principal variables in this situation (which we may consider as unknowns, from the jammer-location point of view) are the number of separate jammers, their azimuthal separation, their ranges from the receiving site, their effective radiated powers, and the angular (azimuthal) rates of each of the jammers.

When conditions are good--few jammers, well separated in azimuth, all producing roughly equal signal strengths at the receiver--a human

operator can count the number of jammers and estimate their azimuths with ease, and (as discussed in Section I) a computer can be programmed to perform the same function as well as, or better than, a human. As the jamming situation becomes more complex, the problem rapidly becomes intractable if the human or the machine only has power-versus-azimuth information.

The basic information desired from the direction-finding system is the number and azimuths of all the jammers; azimuthal rates might be helpful if available. The way in which the systems fail is a complicated function of all the jammer parameters, and even the definition of "failure" is not clear. For example, a system might correctly count the number of jammers, but estimate the wrong azimuths; for some situations, a correct count might be very much more important than the directional measurements. Or the system might correctly measure a few jammer azimuths, but grossly overestimate the number of jammers, and thereby produce numerous completely false reports; perhaps for certain tactical scenarios the availability of some correct data outweighs the presence of other extraneous reports.

With this model of the problem in mind, it is clear that even the unsophisticated constant-amplitude noise jammer represents a severe threat to a jammer-location system if enough jammers are simultaneously within line-of-sight of the system. The enemy can also employ tactics which add to the natural complexity of the situation--he can organize groups of jammers into "clumps" so that their effects tend to augment

one another in azimuth, he can arrange their trajectories so that their azimuths occasionally coincide, he can place them at widely varying ranges to the receiving site, he can cause whole groups of jammers to turn on simultaneously (to obscure time-sequence clues), and he can direct some of them to turn off from time to time (to confuse the process of counting jammers). Thus with enough jammers the simplest type of noise-jammer threat can overwhelm and saturate the most sophisticated direction-finding system, if that system is limited to basic measurements of power versus azimuth.

The enemy has additional flexibilities in the design of his noise jammers and the tactics with which they may be employed. One class of jammer is directed specifically against the bistatic correlation system; for ease of presentation, we shall postpone discussion of these special jamming techniques until after we describe the correlation system more fully, in Section III. Another class involves the use of amplitude modulation to exploit weaknesses in systems using power-versus-azimuth measurements. Three such amplitude-modulated jammers are described in the paragraphs below; they are considered to be more sophisticated than the simple "constant amplitude" jammer, and are presented in order of increasing sophistication*:

Randomly varying Amplitude: The jammer is equipped to vary the amplitude of his radiations according to some random program,

*The titles chosen for these techniques are consistent with the jamming threats surveyed in Section IV.

as indicated in Figure 3; it will suffice if the output power is varied over a small number of discrete levels every few seconds. The purpose of the jamming technique is to confuse any direction-finding approaches that attempt to solve for (and subtract out) the power-versus-azimuth contributions from any of the participating jammers.

Amplitude synchronized with radar: The jammer listens to the scanning radar, and modulates his power in synchronism with the radar's scan pattern, as shown in Figure 4. This implies that the jammer has equipment capable of receiving the radar's transmissions and thereby estimating the orientation of the radar's antenna at all times. The jammer must interrupt his own transmissions to provide "look through" for the receiver. The technique allows a single jammer to create the appearance of many jammers at arbitrary azimuths; jamming energy enters the radar through the radar's antenna sidelobes, but is modulated by the jammer to simulate the main-beam antenna pattern. Alternatively, the jammer can turn off when the actual main beam sweeps past, thus thwarting the jammer-location system. This "inverse gain modulation" approach leaves the jammer vulnerable to skin-tracking by the radar, unless other jammers can simultaneously provide cover through the radar's antenna sidelobes. As another variation, the jammer can modulate his power output in such a way that the direction-finding system makes a slightly incorrect estimate of the jammer's true azimuth.

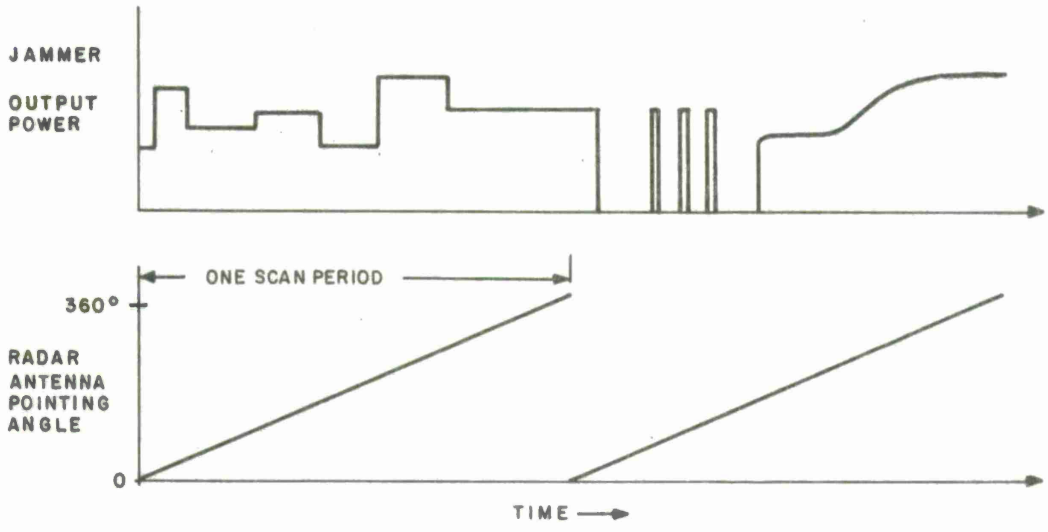


Figure 3 RANDOMLY MODULATED JAMMING

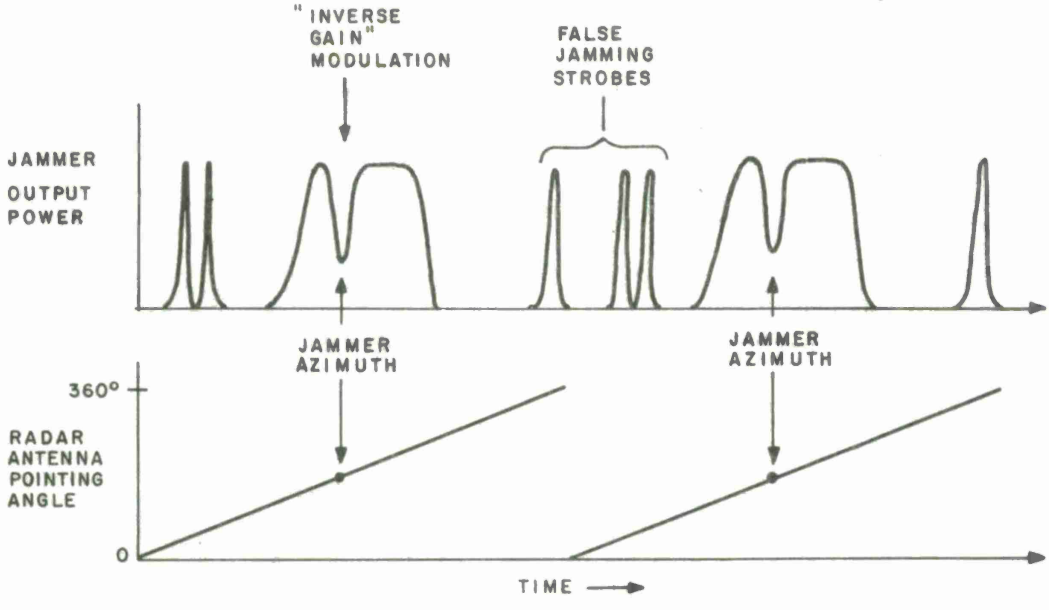


Figure 4 SCAN—SYNCHRONIZED JAMMING

Synchronized modulation is aimed principally at mechanically scanned radars whose scan rate is constant; electronically scanned arrays with constant scan rate are also susceptible.

Cooperative Modulation: Multiple jammers can cooperatively attack a given radar, by synchronizing their transmissions in an efficient way with the scanning of the radar's antenna. Each jammer has receiving equipment with "look through" capability, and all the jammers communicate with one another over a secure data link. The tactic arises from the observation that there is no need (from the standpoint of jammer self-protection) to jam the radar unless the radar happens to be pointing at one of the jammers. Thus all the jammers can remain silent until any one of them judges that the radar beam is about to sweep over him--then he requests one or more of the other jammers to radiate into the radar's antenna sidelobes, as shown in Figure 5. With this tactic, the radar never succeeds in skin-tracking a silent jammer, yet never has the opportunity to measure the direction of an active jammer. As with the previous threat, the jammers can easily create the appearance of many false jammers.

Having described four different noise-jamming threats, we shall now turn our attention to a variety of direction-finding systems designed to cope with one or more of these threats, as well as some more sophisticated jamming techniques.

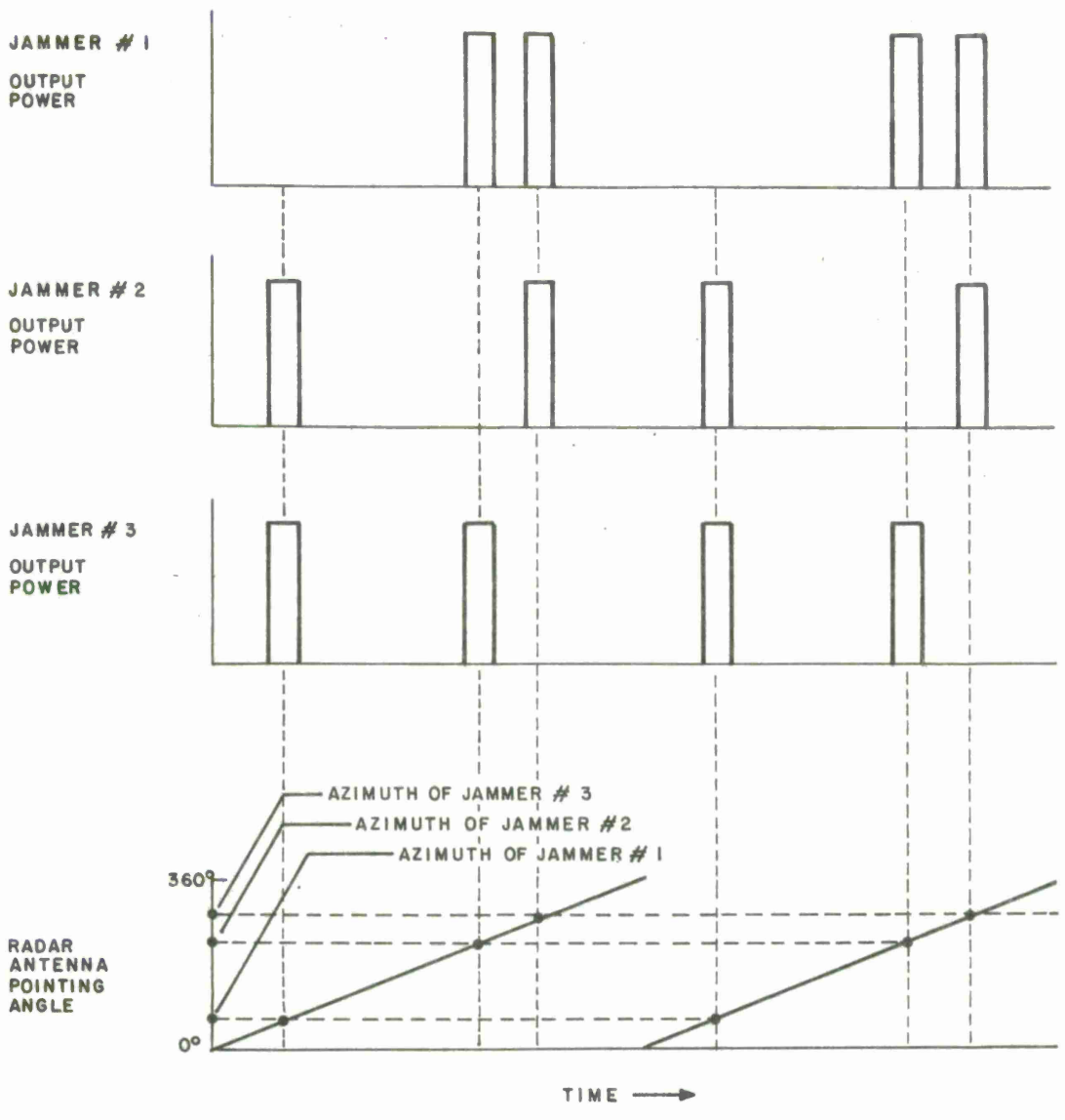


Figure 5. EXAMPLE OF COOPERATIVE JAMMING

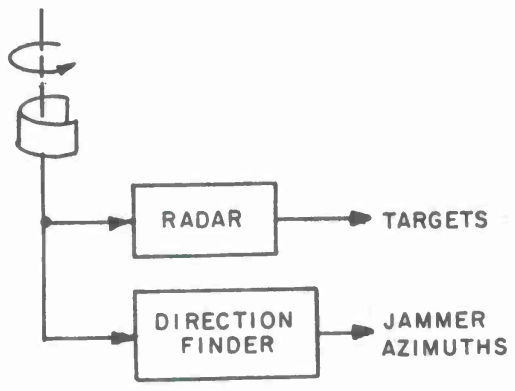
SECTION III

DIRECTION-FINDING AND JAMMER-LOCATION TECHNIQUES

In this section we shall discuss six approaches to the problem of locating amplitude-modulated noise jammers. Five of the techniques attempt to measure the azimuths of the jammers, and several sites must be netted together to locate the jammers by triangulation. The sixth approach, bistatic correlation, involves two sites and is capable of locating jammers in both range and azimuth. The first four systems are closely related and utilize power-versus-azimuth measurements in a variety of ways. Our discussions are arranged in order of increasing system complexity and cost.

System No. 1

The simplest of our techniques uses the radar antenna to collect all of the measurements. It is desirable to use a separate receiver to process the jamming signals, rather than use the radar receiver, because the requirements for the two functions are generally much different: The radar needs maximum sensitivity, and can vary the receiver gain as a function of range, to ease the dynamic-range requirements; the jamming processor is not particularly concerned with sensitivity



or noise figure, but must retain an extremely large dynamic range at all times.

The equipment* for direction-finding can be implemented easily, as shown in Figure 6. The average-power estimates are sampled frequently, converted to digital form, and submitted to a general-purpose computer for analysis. There need be no special relationships between the sampling rate and the radar's timing; the only requirement is to provide enough samples of the power-versus-azimuth pattern to permit the computer to interpolate accurately. All of the complexity in the system lies in the computer software.

As discussed earlier, the appropriate computer algorithms have not been developed, except for simple cases. One approach to their design is to emulate the human operations of adaptive pattern-recognition, although this is not necessarily the optimum procedure. When faced with a group of constant-amplitude noise jammers, an algorithm that correlates the measured amplitude-versus-azimuth function against stored replicas of the antenna pattern would seem to hold promise. However, limited numerical experiments with this approach have been disappointing, because the sidelobes of the radar antenna can occasionally show a strong resemblance to the main-beam region, and many false correlations are reported. The algorithm can be augmented by exploiting the one-at-a-time

*It should be noted that this simple equipment is all that is necessary to implement an automatic version of the Threshold Control Unit (see footnote on Page 8).

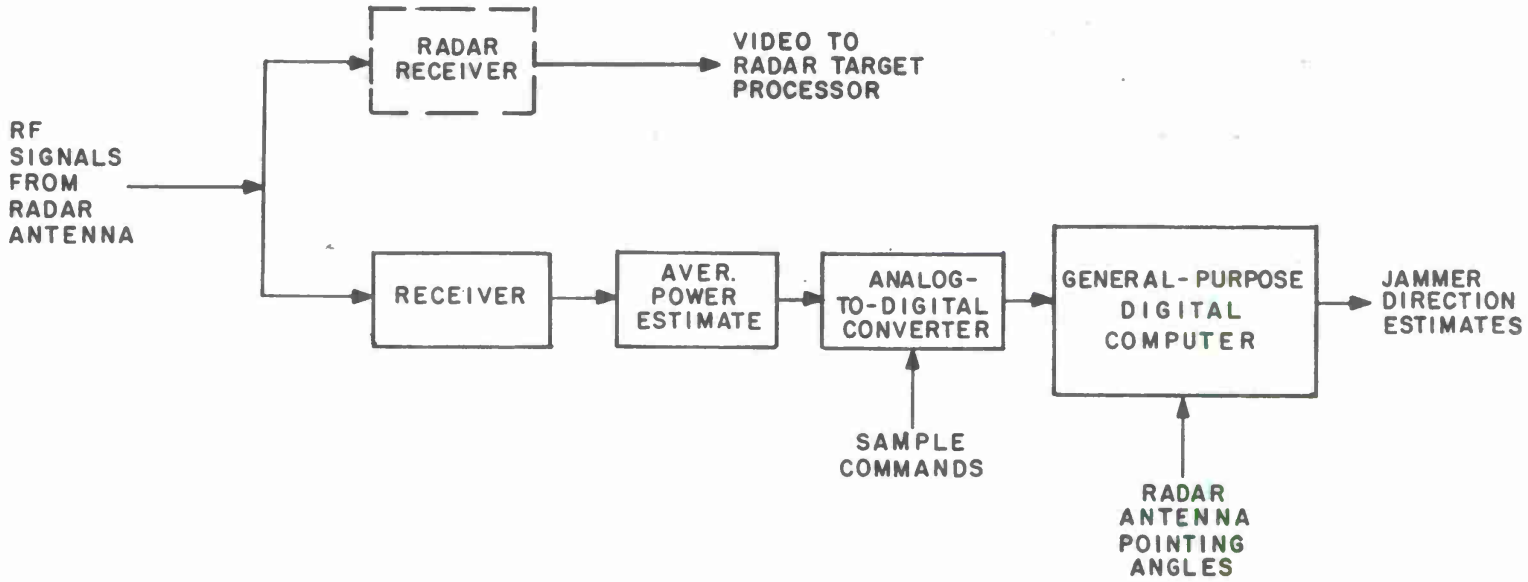


Figure 6. DIRECTION-FINDING EQUIPMENT FOR SYSTEM NO. 1

appearance of new jamming signals, and subtracting the contributions of those jammers which have already been recognized and measured. Difficulties will be encountered if the radar antenna's pattern changes appreciably as a function of the direction in which the main beam is pointing; it is probably necessary to store many different versions of the antenna pattern.

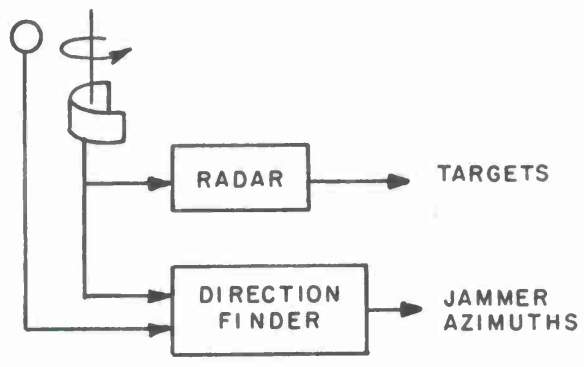
Algorithms are available which will work reasonably well in specific situations, e.g., threats which are constrained to lie within fixed range intervals, all with equal unmodulated noise power, distributed favorably in azimuth with respect to the receiving site. These simple algorithms will fail if the number of jammers or their geometrical relationships are unfavorable. Considerable development and experimentation is required to produce computer algorithms which can adequately handle the general case of the simplest (constant-amplitude) noise jamming threat. No amount of clever programming will enable the system to perform well against the more sophisticated jamming threats--the measured information is too limited, and the enemy has too many degrees of freedom, to effectively sort out the jammers' positions.

The above comments apply primarily to a mechanically scanned radar, whose constant scan rate is observable and exploitable by the enemy. An electronically scanned phased-array radar, however, has the potential for avoiding some of these problems. If the beam of the antenna were programmed to move randomly through the surveillance volume, then the enemy could not modulate his jamming power in a synchronous manner.

However, there are two reasons for using a conventional constant-rate scan pattern for surveillance, even if the potential for random scanning is available to the phased array. First, most radar-processing programs are based on a constant update rate; this is not a fundamental issue, but in fact virtually all such programs are written with an essentially fixed frame-time. Second, the radar cannot beam-split in azimuth unless it has at least two adjacent beams overlapping each target; random surveillance is wasteful of power because more beams would be transmitted to support beam-splitting than would be needed if constant-rate scanning were used. Although an agile-beam radar could provide better immunity to synchronized jamming, the authors know of no operational phased-array system that actually delivers this advantage in the surveillance mode.

System No. 2

This system is similar to the previous version, in that it uses the radar's antenna to measure jamming power versus azimuth. Additional information is made available through a separate "guard" antenna, as shown in Figure 7. Against some jamming threats the direction-finding performance will be improved.



The radar's antenna pattern may be divided into two regions: the high-gain beam and its nearby large sidelobes, and the "far" sidelobes

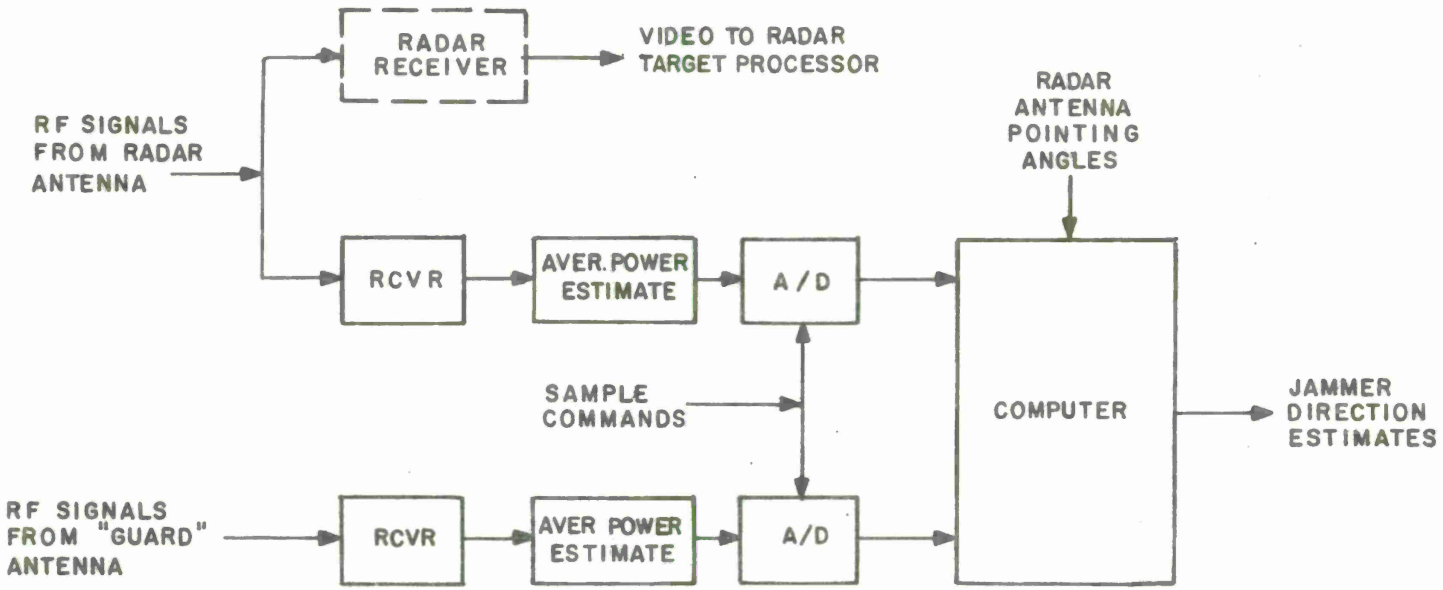


Figure 7. DIRECTION-FINDING EQUIPMENT FOR SYSTEM NO. 2

which are normally 20 dB or more below the first region. The gain of the guard-antenna channel is adjusted so that the output of the guard receiver is less than the radar's when a signal source (a target or a jammer) is in the main beam of the radar, but greater when the source is outside the main beam. Hence, for simple situations we may determine whether a source is in the main beam of the radar or not by examining the relative output from the two channels.

For direction-finding purposes, the guard antenna can provide clues to the computer algorithm that may improve the system's performance in some cases. When a single jammer attempts to deceive the system by injecting false strobes through the radar antenna's sidelobes, the guard antenna will permit the computer to discard the false reports. For more complicated situations, the guard-channel output must be used with caution, because complete reliance on its ability to distinguish main-beam signals from sidelobe signals can actually decrease overall system performance.

If the enemy has one small jammer in the main beam of the radar antenna and several strong sources injecting noise through the sidelobes, then the total power entering the guard antenna may be nearly as large as the power coming through the radar antenna. Because the guard antenna is only a coarse approximation to the radar antenna's sidelobe pattern, the power ratio between the two receiver channels may fluctuate considerably, depending upon the precise alignment of the sidelobe pattern with the jammers' azimuths. Thus when the ratio

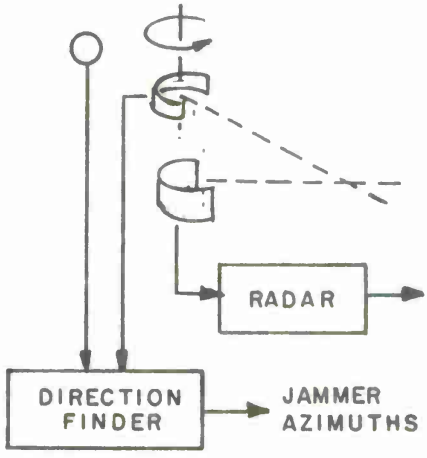
is nearly unity, the computer algorithm will have difficulty deciding whether or not to ignore the presence of the main-beam jammer.

Whatever advantages the guard antenna confers to the system may be enhanced by using a more complicated antenna. Ideally, the guard pattern should be an exact lobe-for-lobe match to the radar antenna's sidelobe pattern. While this would be extraordinarily difficult to achieve in practice, the guard pattern can be designed so that its gain approximates a smoothed version of the main-antenna pattern; the guard antenna must now rotate in synchronism with the radar antenna. If the detailed pattern of the radar antenna changes significantly as it rotates, the guard antenna must be designed for the average case, or must somehow be made to alter its characteristics with rotation.

The guard antenna is a valuable addition to the system, but does not improve matters much in complex jamming situations.

System No. 3

The third system approach is a minor variant on the second. The required equipment is shown in Figure 8. Rather than using the radar antenna itself to measure power versus azimuth, the direction-finder obtains its signals from a separate antenna which is mounted on (and rotates with) the radar antenna.



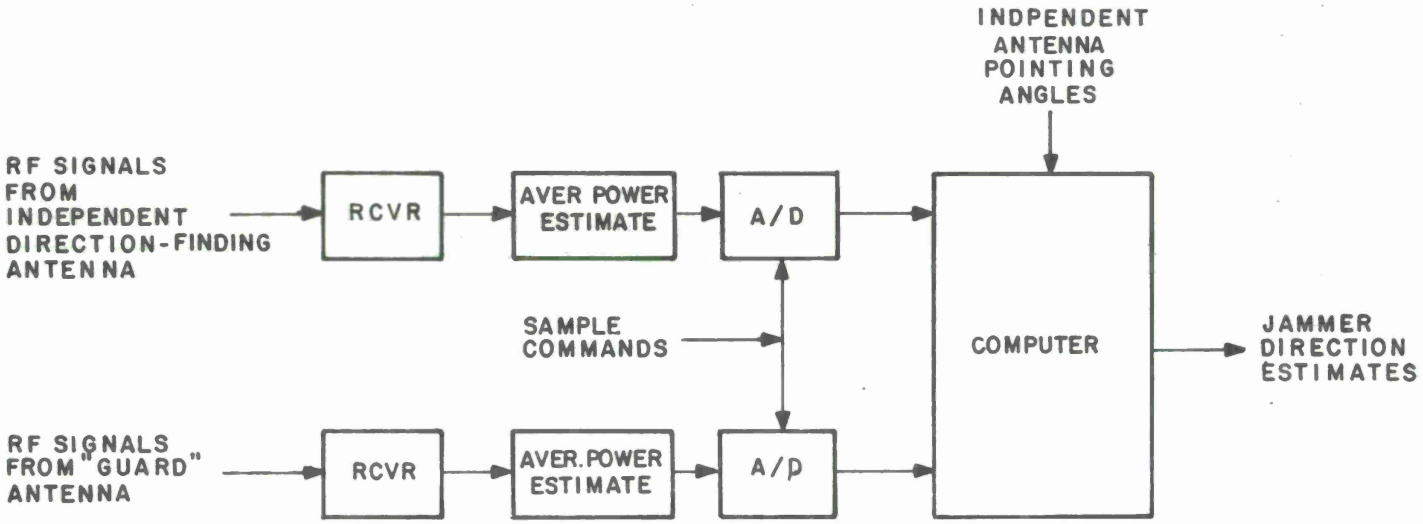


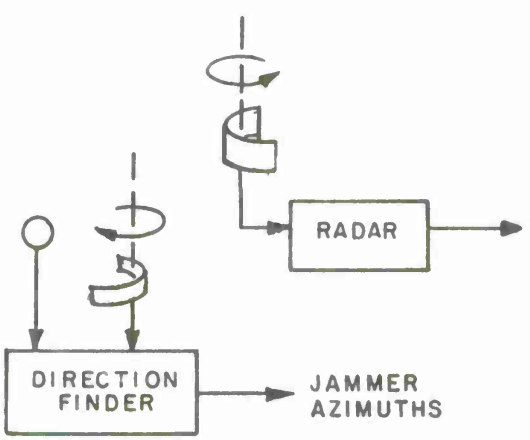
Figure 8. DIRECTION-FINDING EQUIPMENT FOR SYSTEMS NO. 3 AND 4

The separate antenna is arranged to have a different boresight angle from the main antenna; i.e., the separate antenna may be mounted back-to-back with the radar dish, or may be squinted 20° or 30° from the main beam of the radar. The difference in the two boresight angles is kept secret from the enemy. If the enemy does not know the difference in angle between the main beam and the (passive) direction-finding beam, he cannot exploit some of the modulation techniques that are otherwise relatively simple--in particular, the "inverse gain modulation" tactic is no longer valid.

Other jammer-modulation threats which depend only upon synchronism with the radar's scanning rate are still troublesome, because the scanning rate of the separate antenna is identical to the main antenna, and can be observed and measured by a distant enemy.

System No. 4

This is the first in our series of system approaches that is entirely independent of the radar. The direction-finding system site can even be located at a different site from the radar, if desired.



Although the method relies on amplitude-versus-azimuth measurements, and suffers from the general limitations discussed

earlier for this class of system, the independent antenna offers many advantages against the more sophisticated jamming threats. Since there is now no fixed relationship between the scanning rates and pointing angles of the radar antenna and the direction-finding antenna, the enemy cannot benefit from tactics that rely on such relationships. Furthermore, the scan rate of the direction-finding antenna can be very much higher than the radar's, giving the system an opportunity to detect and measure the power from jammers that wink on and off rapidly. The processing equipment is shown in Figure 8.

The cooperative jamming threat is an especially severe problem in general because--as discussed in Section II--it permits a group of cooperating jammers to jam the radar, and yet not permit the radar to determine the directions to the jammers. The tactic can succeed easily with a conventional radar, because each jammer simply turns off whenever the radar's main beam sweeps by. To be effective, the cooperative jammers in the radar's sidelobes must turn on for at least the normal illumination time of the radar; i.e., they must jam at least as long as it takes the radar's main beam to pass over the target (or else the silent jammer will be skin-painted in the main beam of the radar).

If the independent antenna of our No. 4 direction-finding system rotates rapidly enough, we can be assured that even the winking cooperative jammers will be detected at their true azimuths; this does not necessarily allow us to eliminate all the ambiguities and confusions

associated with multiple jammers, but it would help enormously in the basic measuring process. Unfortunately, this requirement implies a rather high-speed antenna. For example, if the radar has a 6° azimuthal beamwidth and rotates once in ten seconds, then the illumination time is 1/6 second; if our direction-finding antenna rotates once during the illumination time, it must revolve at 360 RPM. Narrower radar beamwidths make the design problem more severe.

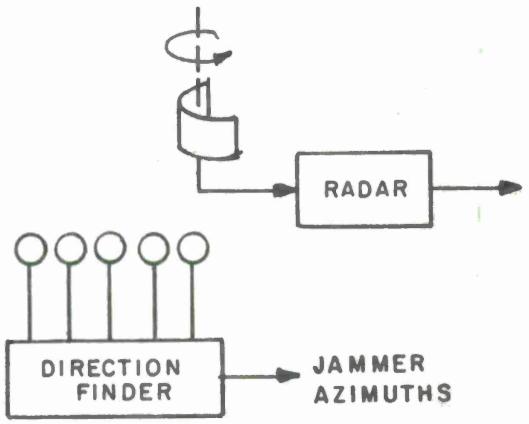
We can meet the rapid-scan requirement in several ways. First, the direction-finding antenna could be small, to facilitate a direct mechanical solution. The azimuthal resolution of the antenna would then be much poorer than the radar's, and the ability of the system to perform raid-counting and other related operations would be impaired. The introduction of a slow high-resolution antenna, perhaps rotating with the radar antenna but pointing in a different direction, could provide a backup to the coarse rapidly scanning direction-finding system.

A second way to meet the rotation speed requirement is to implement a number of antennas and their corresponding receivers, and scan them in the manner of a multi-bladed fan. A third method is to fabricate an electronically scanned array, which is probably the most satisfactory approach since its scan rate could be variable and as high as desired. The array would be passive and need not support a good receiver noise figure, and thus could be constructed at fairly low cost; strip-line techniques might be appropriate for this task.

If the independently rotating antenna has a high scan rate, but not high enough to meet the illumination-time requirement, the system still has merit because there is a finite probability that the scanning antenna will accidentally be pointing at a modulating jammer at the moment the jammer decides to turn on. For some scenarios the detection probability may be large enough to warrant the extra expense of the system.

System No. 5

The previous four systems relied on, or were limited to, measurements of jammer power. System No. 5 is an electronic array capable of measuring the amplitude of received signals, and therefore can hope to bypass many of the deficiencies inherent in the power-only approaches.



The direction-finding array is not, in the usual sense, a phased antenna at all. It does not steer, and no main beam or nulls are created. Rather, it is merely a collection of independent passive omni-directional receiving elements, whose purpose is to receive jamming signals from a variety of different locations relative to the jammers. The amplitude and phase of the received signals are measured at each element, and the results are digitized and sent to

a general-purpose computer. The computer solves several sets of simultaneous equations, and finally produces the desired azimuths of the jammers.

The authors are not aware of any work, either theoretical or experimental, directed toward this basic approach. Bark has suggested a particular implementation and has performed a limited analysis of its properties. Figure 9 shows a diagram of the analog operations associated with a portion of the array. The received signals at each element are first heterodyned down to two quadrature low-pass channels, and then are cross-correlated with the corresponding outputs from other elements. The cross-correlation operation is taken over an averaging time T, and thus is not affected by any jammer modulations or waveform complexities over this time period. The interval T is chosen long enough to achieve the desired sensitivity, but not so long that the jammer aircraft can move appreciably in azimuth. For an array of N elements, the computer is furnished 2N measurements (digital numbers) every T seconds. The computer must execute a straightforward algorithm to find the unknown jammer azimuths, and no high-speed computations appear to be required.

The practical questions of mechanical tolerances, numerical accuracy in the measurements, the response pattern of the individual elements, etc., have not been answered to date. Although the array is not "adaptive" as described, it may be necessary in practice to feed back preliminary data to the analog processors at each element,

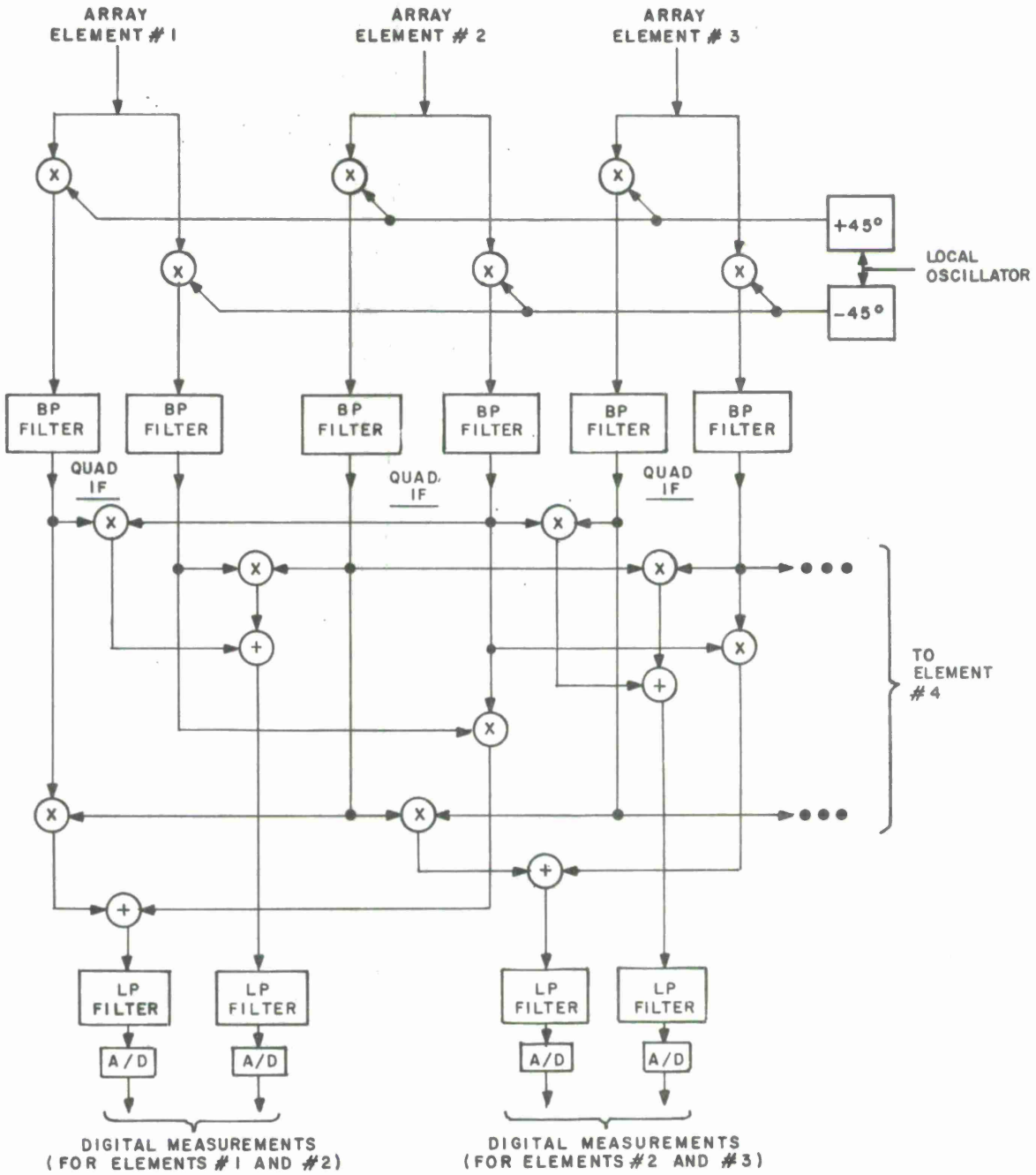


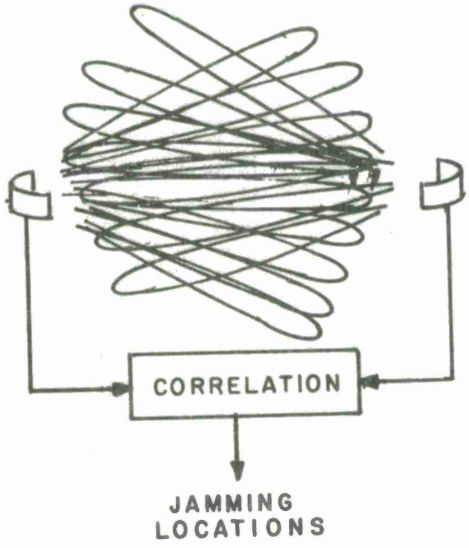
Figure 9. PART OF EQUIPMENT FOR DIRECTION-FINDING SYSTEM NO. 5

where the amplitude and possibly the phase can be adjusted to ease the dynamic-range requirements in the cross-correlators. The array itself could be relatively inexpensive, since it is passive; a printed-circuit implementation seems especially appropriate at the primary radar surveillance bands (L and S).

It should be noted that the direction-finding array could be used to steer the nulls of a phased-array radar (or of several sidelobe cancellers) to improve the radar's performance as well as locate the jammer.

System No. 6

The bistatic correlation approach is the only one examined in this report that has the potential for locating multiple jammers in both range and azimuth, without the production of "ghosts". However, it is also the most expensive of all of the alternatives.



Correlation systems measure another parameter in addition to angle or power-versus-azimuth information. This parameter is the path-length difference from the jammer to two sites which are separated from one another by tens

of miles. The measured path-length difference places the jammer on a hyperbola*, and the jammer's actual location is defined by the intersection between the hyperbola and at least one angle as measured by a directional antenna.

Some simple configurations using a rotating directional antenna at one site and an omni-directional antenna at the other have been analyzed and tested, but they are so limited that we shall not consider them further. Instead, we shall discuss a system that employs stationary multi-beam antennas at both sites, as shown in Figure 10. The wideband IF signals received by each antenna beam at the secondary site are sent over a microwave link to the primary site for correlation processing.

Let us assume that the signal from a single jammer is received at the two sites; except for amplitude, time delay, and doppler shift the two received versions of the signal are identical. If we bring the two signals together at the primary site and subject them to the processing shown in Figure 11, then the output will show a maximum when the time delay τ is adjusted to be equal to the time difference between the two paths to the jammer. The measured value of τ then locates the jammer on the appropriate hyperbola.

---

*The locus of a constant time (range) difference is a hyperboloid, but we are dealing here with an essentially two-dimensional situation so long as the jammers are relatively far away.

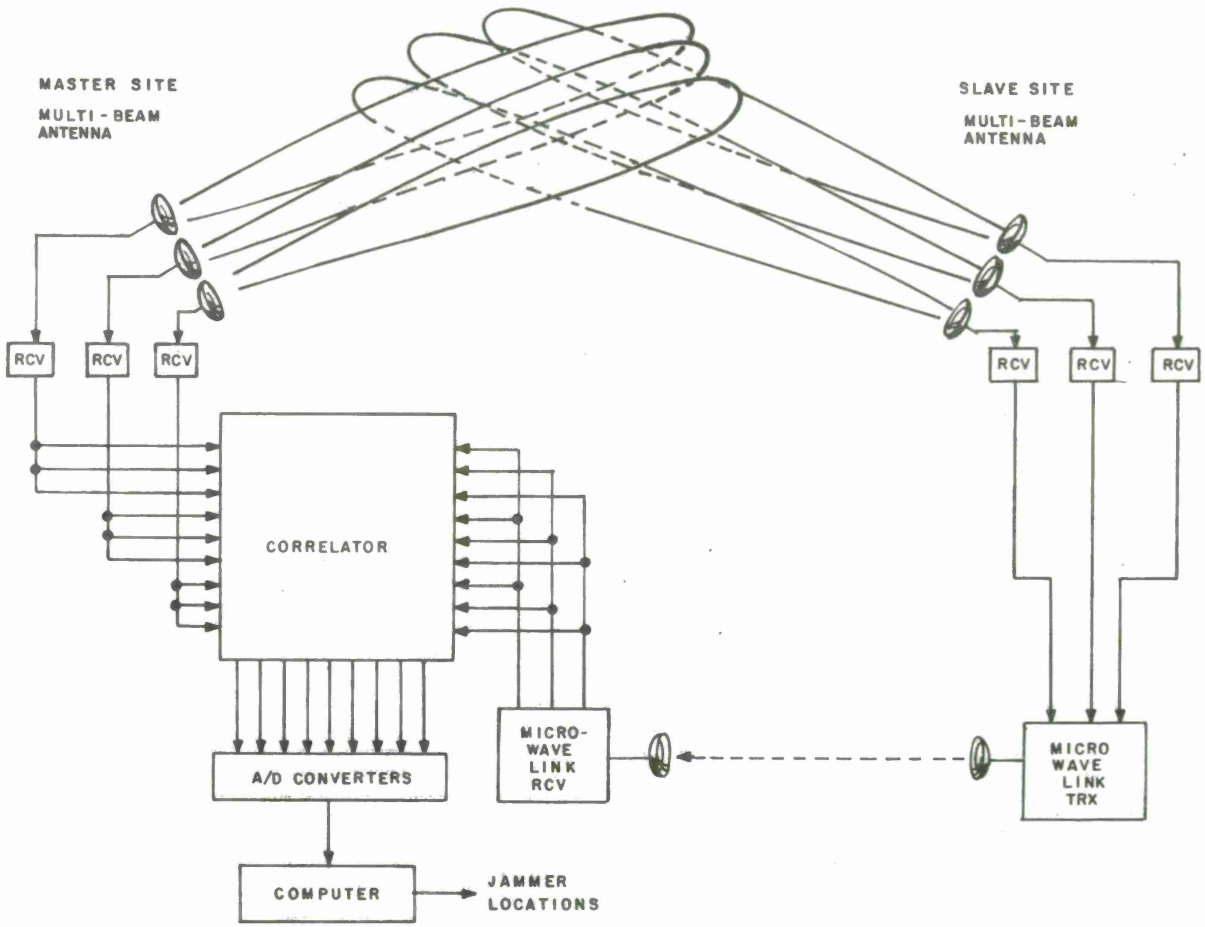


Figure 10. BLOCK DIAGRAM OF BISTATIC CORRELATION SYSTEM NO. 6

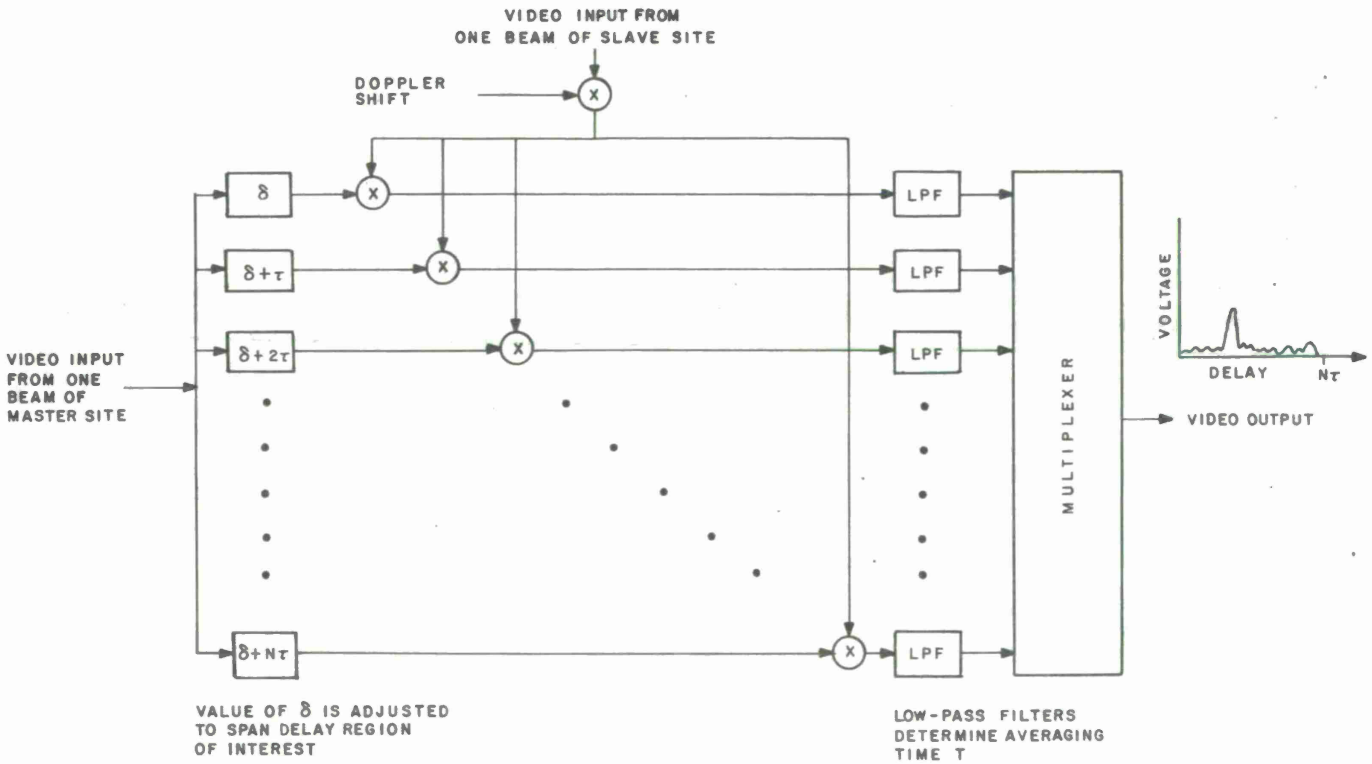


Figure 11. BLOCK DIAGRAM FOR SINGLE-BEAM CORRELATOR

The performance of the system is a strong function of the bandwidth W of the correlated signals and the time T over which the correlation product is averaged. Since this is a passive system, W is basically a property of the jammer's radiation; but in practice, the bandwidth restrictions of the microwave link will set the upper limit to the effective correlation bandwidth. The averaging time T is determined by the anticipated speed of the jammers--the faster they move, the shorter the available integration time. It should be noted that the integration time may also be limited by the length of time the jammer is turned on, as with "winking" cooperative jammers. The product TW is one measure of the system's ability to separate signals from multiple jammers.

In a complex jamming environment, it is likely that all of the multiple-antenna outputs will contain significant power from all of the jammers. However, as long as the system is designed to achieve low sidelobes in the correlation (time) domain, it will be possible to distinguish among main-beam and sidelobe jammers by examining the correlator outputs. The algorithms for counting the number of separate jammers and for estimating their locations are based on straightforward amplitude and time decisions, and are easily automated.

The multi-beam antenna configuration does not scan, and consequently is not susceptible to the amplitude-modulated threats described in Section II. Furthermore, the combination of antenna gain and substantial signal-processing gain makes the system highly resilient, permitting

good unambiguous performance even when confronted by large numbers of jammers with unfavorable power ratios. The use of doppler processing can even give some direct information about the speed and direction of the jamming aircraft.

Three different jamming techniques have been identified as possible countermeasures against the correlation system. In the first, the enemy radiates a special pseudo-random noise which has a repetitive structure. When this noise is processed by the system, multiple values of delay τ can be found which cause the correlator's output to be a maximum. Thus the specially designed noise generates ambiguities within the system. The concept can be extended by having multiple jammers all radiating the same pseudo-random waveform. Second, the enemy's jamming aircraft can be equipped with two directional antennas, as shown in Figure 12. The antennas are connected to two different jamming transmitters, and are pointed at the two bistatic sites, so that each site receives different noise. Under these conditions the correlation process will fail to detect the jammers. The third jamming technique calls for the installation of a series of antennas on the enemy aircraft, each radiating noise which is uncorrelated from the others, as shown in Figure 13. If enough antennas are used, the jammer will appear as a distributed source, and will not correlate properly in the jammer-location system.

These three techniques are specifically directed against the correlation approach, and presume that the enemy knows the parameters

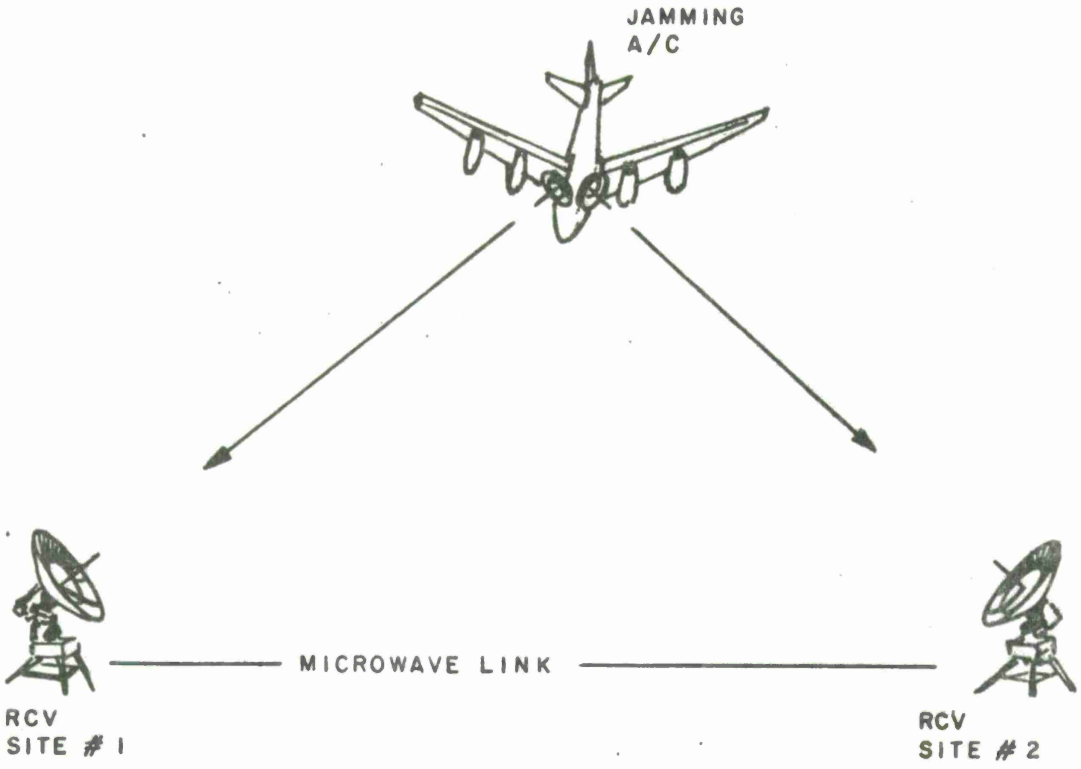


Figure 12. DIRECTIONAL ANTI-CORRELATION JAMMING

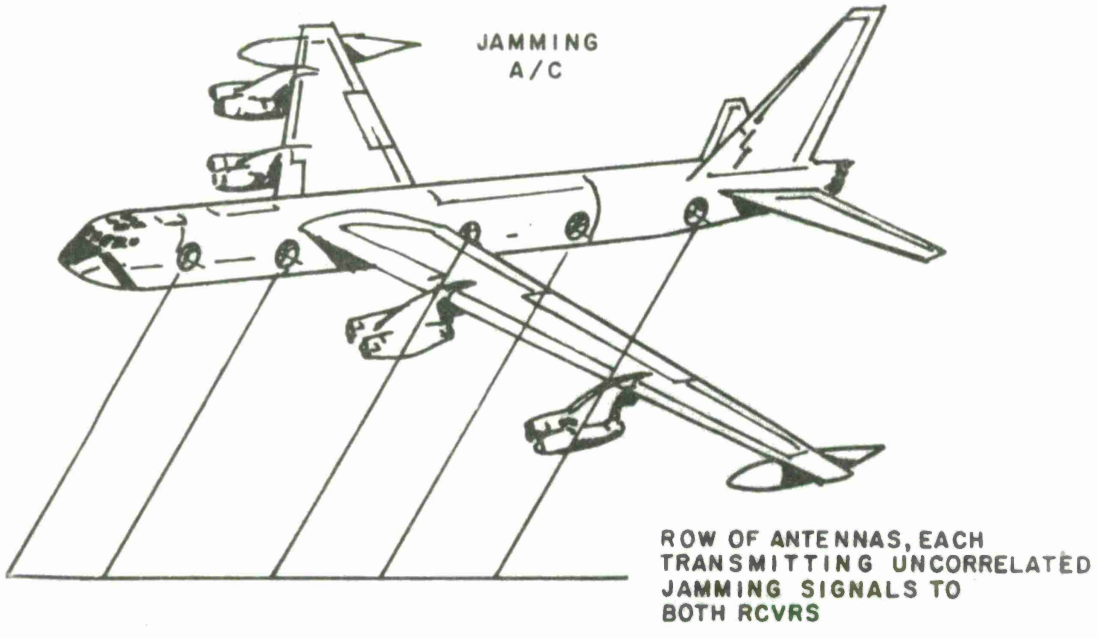


Figure 13. "DISTRIBUTED" ANTI-CORRELATION JAMMING

of the system and has sufficient interest to develop responsive countermeasures; however, it is acknowledged that all three techniques also can be operated efficiently against conventional radars and direction-finders. The first (multiple-correlation pseudo-noise) is expensive for the enemy, since it implies the use of a power-amplifier chain in the jamming transmitter. The two-antenna technique has the problem of finding and pointing at the two receiving sites; the undesired cross-radiation must be suppressed by as much as 40 dB to overcome the correlation gain of the location system. The distributed-source technique requires many antennas and jamming transmitters, and is likely to be correspondingly expensive.

Two Additional Location Techniques

Two more techniques for measuring jammer azimuth have been devised*, but they will only be mentioned briefly because they have not been studied in any detail and do not appear to offer any substantial improvements over the other approaches.

As noted in the discussion for System No. 1, the sidelobes of a conventional antenna are often locally similar to the main-beam region, and it is easy for the direction-finding system to confuse weak main-beam jammers with strong sidelobe jammers. A possible improvement may be obtained by designing a special antenna for direction-finding

*These two techniques were identified and described by A. Bark. He believes that he learned of the concepts many years ago, but cannot recall their origin and has not located any supportive literature.

purposes: The antenna has no main beam (essentially omni-directional) and its sidelobes are deliberately made random, so that one portion of the pattern cross-correlates poorly with any other portion. If such an antenna is rotated fairly rapidly, and is used to receive jamming signals, a straightforward correlation of the power-versus-azimuth function with a stored replica of the random-sidelobe antenna pattern should yield a reasonably good measure of the jammer azimuths.

A second unexplored technique for direction-finding utilizes a pair of omni-directional antennas mounted on a cross-bar, as shown in Figure 14. The whole assembly is whirled around at high speed. The relative motion of the two antennas imposes Doppler shifts on the received jamming signals. The amount and direction of the Doppler shift at any given moment is a function of the jammer's azimuth. Suitable processing of the two received signals can, in principle, reveal the azimuths of multiple jammers.

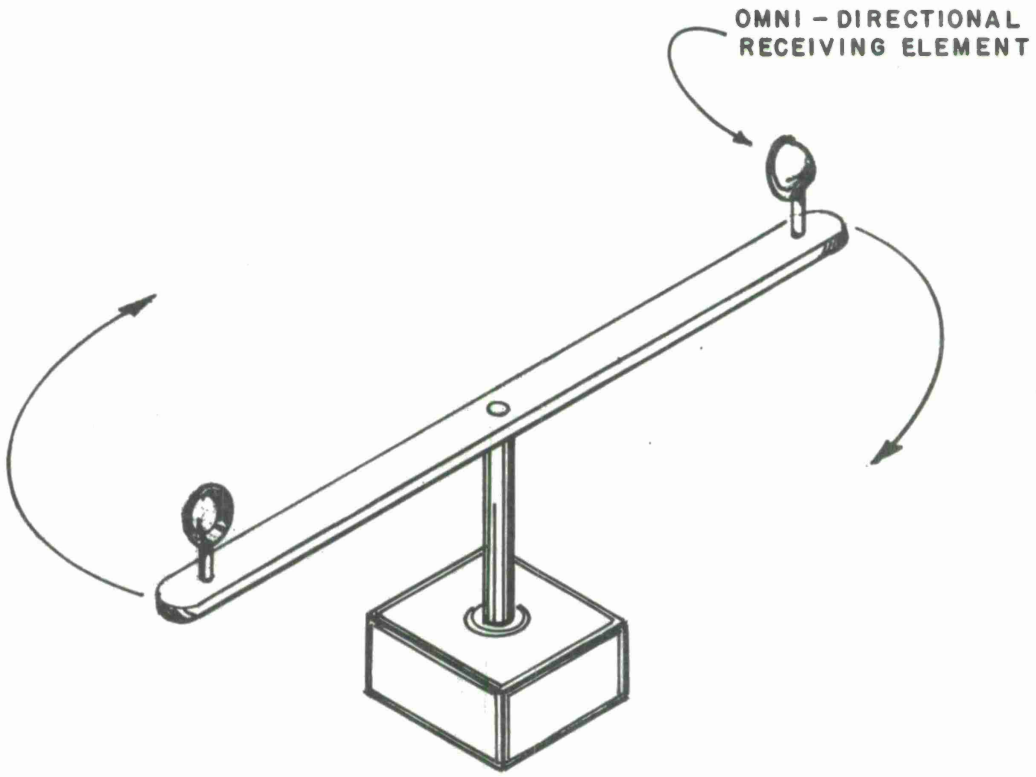


Figure 14. ROTATING DUAL-ANTENNA ASSEMBLY FOR DIRECTION FINDING

SECTION IV

SYSTEMS VERSUS THREATS

Despite the limited scope of this survey, it is evident that direction-finding is a complicated subject. It is difficult to quantify the performance of any of the systems when operating against multiple jammers, because the measures of performance in such situations are rather vague and the behavior of the systems has not been studied adequately, especially under realistic operational conditions.

In an attempt to clarify the relationships among the various system alternatives and jamming threats, we have ranked the systems and the threats according to technical sophistication, which is related monotonically to system complexity and cost. The ranking is presented as a 6 x 4 matrix in Figure 15, showing relative performance for each of the 24 system/threat combinations.

The performance matrix is intended to be helpful to the system designer who is concerned with both radar surveillance and jammer location. It can be used as a guide in making decisions about the type of jamming threat the system should be capable of handling, and the location approach which yields the best performance consistent with other design constraints. However, the matrix must be used with caution, because it can be interpreted properly only if a complicated tangle of caveats and interrelationships have been digested by the reader. The remaining portions of this section will review the basis for rankings and performance ratings shown in Figure 15.

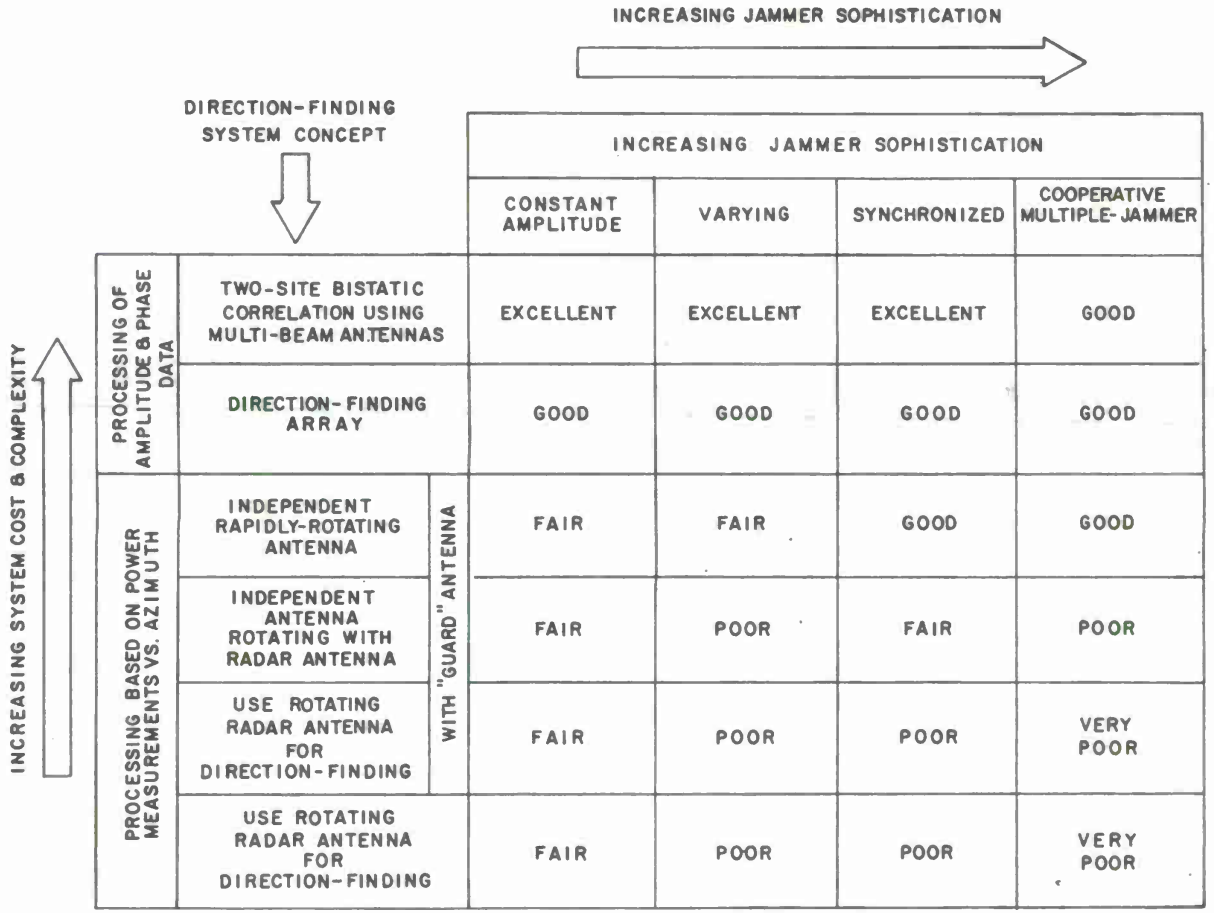


Figure 15. PERFORMANCE OF VARIOUS SYSTEMS VS. AMPLITUDE-MODULATED NOISE JAMMERS

General Caveats

The matrix deals with amplitude-modulated noise jammers, and does not address the whole class of deception and spoofing jammers. Only conventional noise jamming is considered here; special pseudo-random correlated-noise jammers directed against systems Nos. 5 and 6 are ignored on the chart.

The jammers are assumed to be working against a network of conventional mechanically scanned radars whose scan rate is constant.

Systems Nos. 1-5 are capable of measuring only the azimuth of enemy jamming aircraft. It is necessary to bring measurements from two or more sites together and employ triangulation algorithms (presumably in a central computer) to locate the jammers. This process can generate "ghosts". Various methods for extracting unique tags or identifiers can be used at the direction-finding sites to help alleviate the ghost problem, but the methods and their potential are not considered in the performance ratings for the matrix. System No. 6 inherently avoids ghosts.

The two additional direction-finding techniques mentioned at the end of Section III are not included here.

Relative System Costs

The six location techniques are listed in order of increasing sophistication, complexity, and cost, but this ordering is not necessarily correct under all circumstances, as discussed below.

Since System No. 2 represents a hardware addition (the guard antenna and its processor) to System No. 1, and most likely requires more complex computer algorithms, System No. 2 should always be more expensive. Similarly, System No. 3 is obtained by adding a third independent antenna, or by modifying the radar antenna so that an equivalent independent channel is achieved. The significant technical problem is to squint the beam of the direction-finding antenna with respect to the radar antenna's boresight by an angle which is unknown to the enemy; this requirement suggests an arrangement which could be adjusted in the field to maintain long-term secrecy. Depending on the design, an independent squinted-beam antenna could be inexpensive or might be a substantial fraction of the radar antenna's cost. The requirements for azimuthal resolution will play a large part in determining the cost. At any rate, the relative cost of System No. 3 should always be greater than System No. 2.

The cost of System No. 4 can vary over wide limits, and might possibly be less than System No. 3 for some versions. The requirement for an independent rapidly scanning antenna is probably best met with a passive phased array. If such an antenna could be constructed with printed-circuit techniques, and if the desired azimuthal resolution permits the structure to be fairly small, then the overall cost might be low; otherwise, the device is rather elaborate and correspondingly high in cost. System No. 5 uses another array-like structure. No firm equipment designs have yet been attempted, but the concept

calls for precision measurements of amplitude and phase at each array element, with independence from the jammers' signal strength and modulation tactics. Consequently, it is assumed that the hardware costs for the array and its processing equipment may be substantially higher than for System No. 4.

Real-world experience may reveal that both Systems Nos. 4 and 5 are less difficult to fabricate than System No. 3, despite their apparent complexity. It should also be noted that Systems No. 4 and 5 are completely independent of the radar, and can be placed at different locations; the cost of erecting independent sites, with all the complications implied (prime power, communicating data to the central processor, maintenance, etc.) will in general be much higher.

System No. 6 is ranked as the most costly because it requires at least two sites which must be connected with a wideband communications link--microwave, or fibre optics--and demands high-performance multiple-beam antennas at each site. The correlation processor is also likely to represent a considerable hardware investment.

Relative Jammer Costs

The four noise-jammer threats (A through D) used in Figure 15 are arranged in order of increasing sophistication, and it is clear that this same order applies to cost as well. However, it would appear that threat D is not very much more expensive than the simplest threat A.

The random modulation in threat B calls for a crude variation in effective output power, such as might be obtained with a high-power attenuator, by switching to different antennas or steering a single antenna, or by modulating the power-supply voltages.

Threat C is somewhat more involved, since the jammer must have a "look through" cycle and carry receiving equipment capable of monitoring the signal strengths from the victim radars. These features are probably available to the jamming aircraft already, as part of its general self-defense package. If the jammer intends to use the "inverse modulation" technique, in which the output power is tailored to the strength of the received radar signal (as the radar's main beam sweeps over the jammer), then the accuracy of the power-modulation pattern must be good, perhaps calling for a more expensive modulator design.

Threat D is merely a C-threat jammer that is capable of communicating with his fellow jammers in a multiple-jammer raid. The data link must itself be jam-resistant.

Performance Ratings

The performance ratings from "very poor" to "excellent" are qualitative and imprecise, but are intended to convey an impression of the relative capabilities of the systems. In the paragraphs below we shall discuss the behavior of the six direction-finding systems as they are confronted first by the constant-amplitude jammer, and then by the remaining three jammer types.

Against the constant-amplitude jammer, the performance of the simplest direction-finding system (No. 1) is a strong function of its antenna sidelobes, the number and geometrical distribution of the jammers, and the sophistication of its computer software. In situations where the jammers are well separated in azimuth and few in number, the system may perform quite satisfactorily, but when the jamming environment becomes complex the system responses may degrade in quality until they are virtually meaningless. We have been chosen to characterize this wide range of performance as "fair". The addition of a guard antenna in Systems Nos. 2-4 helps to distinguish among main-lobe and sidelobe jammers in simple situations, but does not offer any real assistance otherwise; in fact, care must be taken to avoid a degradation in performance when using the guard channel. The direction-finding array has been rated "good" in its ability to correctly sort out multiple jammers, because it utilizes extra information (phase) to determine angle-of-arrival of the incoming radiation, and employs signal processing (cross correlation) to help detect weak jammers in the presence of strong. However, these comments are based on theory alone, for the system has not yet been tried in practice. The bistatic correlation system is "excellent" because it avoids the ghosting problem, and combines both antenna directivity and correlation gain to resolve jammers in complex environments.

The randomly modulated jammer degrades the performance of Systems Nos. 1-3 by varying the sidelobe contributions to the total received

signal in a way that confuses pattern-recognition algorithms. The rapidly scanning independent antenna of System No. 4 probably avoids most of this confusion by taking a short time-exposure of the jamming situation, effectively "freezing" the environment. Neither the array nor the bistatic correlator are affected by jammer modulation, since both systems integrate for relatively long periods.

The effects of synchronized modulation are serious to Systems Nos. 1 and 2, because the enemy can determine exactly where the radar antenna is pointing at all times. Thus the "poor" performance rating of these systems against synchronized modulations is even worse than their "poor" rating against random modulation. The synchronized jammer loses some advantage with System No. 3 (he can observe the scan rate, but does not know the pointing angle of the direction-finding antenna), and has no special opportunities against System No. 4. The ratings for Systems Nos. 3 and 4 are slightly better than the corresponding ratings against the random jammer for two reasons: First, the direction-finding computer algorithm can recognize and take advantage of the jammer's synchronism; and second, the signals from multiple synchronized jammers are less likely to overlap in azimuth, and therefore will appear less complex to the system.

The cooperative jammer threat is extremely effective against Systems Nos. 1 and 2, allowing the enemy to jam the radar without being detected by the direction-finding systems. Even though System No. 3 is somewhat independent of the radar's antenna, it is still

possible for the enemy to jam the radar and escape detection most of the time. The high scan rate of System No. 4 makes the detection of cooperative jammers very likely, resulting in a "good" performance rating for our matrix. The direction-finding array and the bistatic correlation system are both capable of good performance against cooperative jammers, since they effectively ignore most forms of jammer modulation. However, the low duty factor "winking" jammers may result in some signal-to-noise degradation, thus weakening the systems' ability to detect weak jammers in the presence of masking interference.

SECTION V

SUMMARY AND CONCLUSIONS

In the twenty years or so since the SAGE system was implemented, relatively little attention has been given to the problem of locating airborne jammers. Many of the techniques developed long ago rely heavily on the skills of human operators, and it is difficult to fully automate these approaches or to quantify the performance of the resulting systems.

Our attention in this report has been limited to barrage-noise jamming. Within this class, the jamming threat has two important dimensions: the number and geometrical distribution of jammers, and the technical sophistication of the jamming techniques. Even the least sophisticated of our threats (constant-amplitude jamming) can represent a severe challenge to a jammer-location system if the number of jammers within view of the system is large. Correspondingly, a single sophisticated jammer can confuse many different types of locating systems.

All of the jammer-location techniques which seem to offer any practical promise for full automation were described briefly, and their relative performance against various forms of noise jamming were presented in a matrix of qualitative ratings. The resulting chart and accompanying discussion, it is hoped, will offer some perspective to the system designer in the form of a "menu" of options,

arranged according to equipment complexity and the severity of the jamming threat.

Considerable work remains to be done, even within the restricted domain of the noise-jamming threat. For those location systems which rely on mechanically scanned antennas, data-processing algorithms for fully automatic operation must be developed and tested against a wide variety of real-world jamming conditions. An important ingredient in the problem will be the accuracy with which the patterns of the ground-based antennas can be measured and stored in a computer.

The direction-finding array is a promising concept, and many design aspects can be taken directly from the field of adaptive-array antennas. However, laboratory and field experience will be necessary to develop a practical system whose performance can be specified quantitatively.

All of the monostatic approaches to jammer-location can be supplemented by the development of on-site processors which measure detailed attributes ("tags") of the received signals, and communicate these signatures to the central processing site. If the individual enemy jammers are measurably different, and if the tag-processors can form reliable indicators of these differences, then the overall system's ability to reject triangulation "ghosts" will be greatly enhanced.

The bistatic cross-correlation approach to jammer location offers good performance at high cost. Some practical experience was gained

with the technique many years ago, but more work is needed to develop an operational system. Recent technology advances in multi-beam printed-circuit arrays and low-cost digital processing elements should have a large impact on the attainable performance of the approach.

The problem of locating jammers which are not in the barrage-noise class is equally important but much more difficult, since the jamming waveforms can vary over a wide range. Nevertheless, whenever the enemy radiates a strong jamming signal he is fundamentally revealing his location, and it should be possible to develop collection systems which can capitalize on this information.